UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/503,282	02/14/2000	Dung Le Huynh	230074-0223	6335

7590 02/23/2004

Ted R Rittmaster Esq
Foley & Lardner
2029 Century Park East
Suite 3500
Los Angeles, CA 90067-3021

EXAMINER	
SONG, HOSUK	

ART UNIT	PAPER NUMBER
2135	16

DATE MAILED: 02/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/503,282	Applicant(s) HUYNH ET AL.	
	Examiner Hosuk Song	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 0203*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-21,23-25 and 43-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-21,23-25,43-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 5,7-8,15,29,35 are rejected under 35 U.S.C. 103(a) as being unpatentable by Wu et al.(US 5,774,551) in view of Candelore et al.(US 6,061,449).

In claims 5,22,35 Wu discloses a control unit having a data input bus (fig.1). Encryption processor in (col.3, lines 58-62). First and second authentication processor in (col.8, lines 61-66). A local data bus, independent of the data input bus to the control unit, coupling the control unit to each of the encryption and authentication processor and a second data bus from the encryption processor to each authentication processor, including a data bus from the first authentication processor to the second authentication processor in (fig.1 #115,109,123 and col.3, lines 56-66). Wu does not disclose where data is provided to at least one encryption processor unit and processed by the at least one encryption processor while at least one authentication processor is further processing output data from one data packet. Candelore disclose concurrent processing in (fig.1 and fig.6). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ concurrent processing disclosed in Candelore with encryption unit disclosed in Wu in order for data packet to continuously flow without delay thus reducing computer downtime. Further concurrent processing allows second packet to be processed quickly thus achieving immediate validation. It overall enhances speed of data processing. Wu discloses control unit controlling encryption processor and authentication processor in (fig.1#115,109). Candelore discloses concurrent processing where first,second and third sets of data are processed in (fig.1). It would have been

obvious to person of ordinary skill in the art to employ pipelining method as taught in Candelore with data processing method disclosed in Wu in order to speed up execution time by ensuring that the microprocessor does not have to wait for the instructions so that when it completes execution of one instruction the next is ready and waiting.

In claim 6, Wu disclose wherein data input bus of the control unit is coupled to a processor bus and each of encryption and authentication processing units comprises a data input bus coupled to the processor bus in (fig.1,#109,123).

In claim 7, Wu discloses first authentication unit and second authentication processor in (col.8, lines 61-65).

In claim 8, Wu discloses all the limitations above. However, Wu does not disclose second data bus comprising a daisy-chain connection between the encryption and authentication processing units. The examiner takes Official notice that chain is well known in the art. It is widely used in order to eliminate conflicting requests to use the channel(bus) to which all the devices are connected, each device is given a different priority.

In claims 15,29, Wu discloses an encrypting a first packet with an encryption processing module and authenticating the encrypted first data packet with a first authentication processing module in (fig.1 and col.3, lines 56-62; col.15, lines 54-67). Wu does not specifically discloses encrypting a second data packet with the encryption processing module while authenticating the first data packet with the first authentication processing module connected to the encryption processing module by a data bus and authenticating the second data packet with the first authentication processing module. Candelore disclose concurrent processing in (fig.1 and col.14,lines 8-12). Anderson disclose concurrent processing method where plurality of packets are processed concurrently for different tasks in (col.11,lines 6-41) It would have been obvious to person of ordinary skill in the art at the time invention was made to employ concurrent

processing disclosed in Candelore/Anderson with encryption unit disclosed in Wu in order for data packet to continuously flow without delay thus reducing computer downtime. Further concurrent processing allows second packet to be processed quickly thus achieving immediate validation. It overall enhances speed of data processing.

Claims 43-46: Wu discloses Encryption processor is disclosed in (col.3,lines 58-62) and at least one authentication processor for data packet processing in (col.8,lines 61-66). Note in (col.15,lines 58-63) discloses that authentication services#109 include DES,RSA and hardware based mechanism such as smartcard. This is a teaching of processor(s) in Wu's system. Wu does not specifically disclose simultaneous data processing. Candelore discloses concurrent processing where first,second and third set of data are processed in (fig.1). It would have been obvious to person of ordinary skill in the art to employ simultaneous data processing method as taught in Candelore with packet processing method disclosed in Wu in order to speed up execution time by ensuring that the microprocessor does not have to wait for the instructions so that when it completes execution of one instruction the next is ready and waiting.

4. Claims 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable by Wu et al.(US 5,774,551) in view of Candelore et al.(US 6,061,449) and further in view of Kocher et al.(US 6,304,658).

Claims 32,33,34: Wu and Candelore does not disclose HMAC-key hashing. Kocher patent disclose HMAC-key hashing method in (col.9,lines 1-16). It would have been obvious to person of ordinary skill in the art at the time invention was made to use HMAC-key hashing method disclosed in Kocher with packet processor system taught in WU and Candelore because HMAC is designed to be resistant to differential analysis. Since HMAC hashes a known value with an unknown value and the result of this hash is then rehashed with a separate unknown value,making any differential attack extremely difficult.

5 Claims 1-4,9-14,16-21,23-28,30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wu et al.(US 5,774,551).

In claims 1-2,9,16,23,30, Wu discloses encrypting and authenticating a first packet and discloses two authentication services connected to the encryption processor by a data bus in (fig.1 and col.15, lines 53-67). Wu does not specifically discloses performing encryption on a first data packet and after completion of the encryption of the first data packet, performing authentication of the first packet and performing encryption of a second data packet prior to completion of authentication of the first data packet. The examiner takes Official notice that encrypting a second packet before authentication is well known in the art. For example, parallel encryption scheme where first and second packets are encrypted at the same time where second packet does not wait for first packet to be authenticated thus allowing faster encryption/authentication process when transmitting over the network or encrypting a second packet before first packet is authenticated or encrypting a second packet while authenticating first packet eliminates waiting time thus enhances encryption /authentication processing speed.

In claim 3, Wu discloses data input bus of the control unit is coupled to a processor bus and each of encryption and authentication processor comprises a data input bus to the processor bus and means for reading and writing data on the processor bus in (see fig.3).

In claim 4, Wu discloses all the limitations above. However, Wu does not discloses second data bus comprising a daisy-chain connection between the encryption and authentication processing units. The examiner takes Official notice that chain is well known in the art. It is widely used in order to eliminate conflicting requests to use the channel(bus) to which all the devices are connected, each device is given a different priority.

In claim 10,17, Wu discloses step of performing a second authentication on the first data packet of data in (col.7, table 1).

In claims 11-14,18-21, Wu discloses appending data to first authentication and second authentication in (col.3, lines 56-66).

In claims 24-28 see claims rejection 10-14 above.

In claim 31 see claims rejection 23 above.

Response to Applicant's Arguments

7. **Applicant has argued that** Wu does not disclose or suggest a plurality of processors,including at least one encryption processor and at least one authentication processor for processing data packets as claimed. **In respone:** Examiner disagrees. Encryption processor is disclosed in (col.3,lines 58-62) and at least one authentication processor for data packet processing in (col.8,lines 61-66). Note in (col.15,lines 58-63) discloses that authentication services#109 include DES,RSA and hardware based mechanism such as smartcard. This is a teaching of processor(s) in Wu's system. **Applicant has argued that** Wu does not disclose or suggest encrypting data from a first packet and communicating an output of an encryption processor to at least one authentication processor. **In response:** Examiner disagrees. Note in fig.1 of Wu's patent shows that computer receives data(packets) from remote computer(135). Although Wu does not specifically use the word packets, data received from remote computer is a form of data packets. Further,#115CPU processes the data and routes the data to number of hardware devices including authenticator/encryptor in #109. **Applicant has argued that** Candelore does not teach processing of multiple data packets. **In response:** Examiner disagrees. Candelore specifically discloses in fig.2 multiple data packet processing.

In view of applicant's arguments on Anderson's patent, examiner withdraws the

rejection based on Anderson's reference.

Applicant has argued that neither Wu nor Candelore teaches data from a second data packet is processed in at least one encryption processor while at least one authentication processor processes data for a first data packet. **In response:** Candelore's patent discloses this process in (fig.6). **Applicant has argued that** Kocher's patent Kocher does not disclose multiple simultaneous processing operations. **In response:** Kocher patent was cited because neither Candelore nor Wu's patent discloses HMAC-key hashing. Sufficient motivation was provided in combining Kocher's reference with Wu and Candelore's references. Further,pipelining method is well known in the art as indicated in the previous claims rejection. **Applicant has argued that** Wu neither discloses nor suggests data buses coupling a control unit and multiple processors,including a data bus coupling one or more encryption processors to authentication processors. **In response:** see fig.1#109,123. **Applicant has argued that** Wu does not disclose a second data bus from an encryption processor to first and second authentication processor. **In response:** Wu's encryption processor and authenticator communicates each other. It would have been obvious to person of ordinary skill in the art to recognize that bus connection is required for communication between the two processors. **Applicant argues that** examiner has cited no prior art in support of Official notice. In response: applicant has not provided any substantial information,evidence or argument challenging the taking Official notice in rejection of these claims. See MPEP 2144.03.

Response to Amendment

4. Applicant has cancelled claims 6,22,36-42.

Claims 1-5,7-9,15-16,29-33 and 35 are amended. Addressed above.

New claims 43-46 have been added. See rejections above.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner can normally be reached on Tue-Fri from 6:00 am- 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100